

Claims

1. Data processing apparatus with

- a local computer unit which correspond to a local data file system for calling and for storing and for bi-directional data transferring of a volume data file by means of a computer unit
- and an user identification unit, which is corresponding to the local computer unit, which enable an access on volume data files through the computer unit by an authorized user as a reaction on its positive identification only,
- whereby the volume data file in the local data file system is stored in a encrypted form, which is not usable for a user

10 characterized in that

- a data transferring path of volume data files between the local computer unit and the local data file system comprise a corresponding key management unit as a part and functionality of the local computer unit, which generate and assign at least one user specific and volume data specific key file for each volume data file,
- the key management unit with a portion of the local data file system, which is connected to the logically separated key database
- and for linking of a key file which is stored in the key database with a volume data file which is stored in a local data file system for generating an electronic document, that is usable by an user
- whereby the key database is provided locally in the data processing appliance and assigned to the local data file system, but logical or structural or physical separated from a drive - or mass storage unit.

25 2. Apparatus as set forth in claim 1, characterized in that the encrypted form comprise the encryption by means of a symmetric key.

3. Apparatus as set forth in claim 1, characterized in that the encrypted form referring of an electronic document as provided on a basis of a volume data file comprise a content - or meaning distorted interchanging, removing or attaching of file components.

30 4. Apparatus as set forth in claim 1, characterized in that the local data file system is a database and the volume data file is a database register or database records of the database.

5. Apparatus as set forth in claim 1, characterized in that the local data file system is a mass storage unit on a workplace with preferable a plurality of users.

5 6. Apparatus as set forth in claim 1, characterized in that the volume data files comprise digital text-, program-, image-, sound- and video files and combinations of these.

10 7. Method for storing and for calling of electronic files, in particular for operating of data processing appliance as set forth in claim 1, characterized by the steps:

- identifying of an user who has access to a computer unit and who has access to a volume data files which is stored on a data file system that is assigned to a computer unit;
- enabling an authorized access on user specific volume data file as a reaction on a positive identification;
- generating of a volume data file and user specific key file for an electronic document that is stored in the data file system and a subsequent linking of the electronic document with the key file for generating and storing of a volume data file, which is not usable for an user;
- storing of the generated key file in a key storage unit;
- reading of a volume data file and user specific key file as reaction on an access command of an user;
- linking of the read-out key file with the volume data file that is given in a non-usable form for an user and that is read-out from the data file system and generating of an usable electronic document.

25 8. Method for encrypting of an electronically stored original amount of data, in particular a method for generating of a volume data file and user specific key file as set forth in claim 7 whereby the electronically stored original amount of data comprise a sequence of information components of a meta language in form of a written language, of a number system or of information component from data elements that are arranged in a predetermined, unitary format structure, in particular image-, sound- or program information and that are stored in a plurality of electronic addressable storage area, comprising the steps:

- Interchanging or removing of an information component in the amount of data or attaching an information component at a predetermined position in the sequence of information components or exchange of an information components with a information component that is preferably not included in the original amount of data

by a computer access on the respective storage area for generating of an amount of encrypted data;

- generating an amount of key data with information on the interchanged, removed, attached or exchanged information component, which is designed in a manner, that a reconstruction of the original amount of data is permitted and
- storing of the amount of encrypted data and storing of the amount of key data in a separated, user specific key file within a common file system.

9. Method for encrypting of an electronically stored original amount of data, in particular a method for operating the key management unit in the apparatus as set forth in claim 1 whereby the electronically stored original amount of data comprise a sequence of information components of a meta language in form of a written language, of a number system or of information component from data elements that are arranged in a predetermined, unitary format structure, in particular image-, sound- or program information and that are stored in a plurality of electronic addressable storage area, comprising the steps:

- Interchanging or removing of an information component in the amount of data or attaching an information component at a predetermined position in the sequence of information components or exchange of an information components with a information component that is preferably not included in the original amount of data by a computer access on the respective storage area for generating of an amount of encrypted data;
- generating an amount of key data with information on the interchanged, removed, attached or exchanged information component, which is designed in a manner, that a reconstruction of the original amount of data is permitted and
- storing of the amount of encrypted data and storing of the amount of key data in a separated, user specific key file within a common file system.

10. Method as set forth in claim 8, characterized in that the successive at least twofold encryption of the amount of key data whereby each is generated with the step of interchanging, removing, attaching or exchanging, whereby a first, hereby generated key data record is assigned to a first user and a second following generated key data record is assigned to a second user.

11. Method as set forth in claim 9, characterized in that the successive at least twofold encryption of the amount of key data whereby each is generated with the step of interchanging, removing, attaching or exchanging, whereby a first, hereby generated key data record is assigned to a first user and a second following generated key data record is assigned to a second user.

5

12. Apparatus for managing an electronically stored original amount of data, in particular for operating the method as set forth in claim 7 with

10

- an analyzing unit, which is designed to access on the original amount of data which are stored in a document storage unit and which is designed to electronically detect at least a sequence of information components of the original amount of data as a reaction on a predetermined or inspected format- or structural data of the original amount of data,

- an encryption unit that is subordinated to the analyzing unit, which is designed for

15

interchanging or removing of information components in the original amount of data or attaching of an information components at a predetermined position in the sequence of information components or exchanging of an information component with an information component that is preferably not contained in the original amount of data and

20

creating an amount of key data with information about the interchanged, removed, attached or exchanged information components, which are designed in a manner, that a reconstruction of the original amount is permitted with key data, and

25

- a storage unit which is designed to store the amount of key data in a key data storage unit and

- a volume data storage unit, which is designed to store the amount of, encrypted data.

30 13. Apparatus for managing an electronically stored original amount of data, in particular as part of the key management unit in the apparatus as set forth in claim 1 with

- an analyzing unit, which is designed to access on the original amount of data which are stored in a document storage unit and which is designed to electronically detect at least a sequence of information components of the original amount of data as a reaction on a predetermined or inspected format- or structural data of the original amount of data,

35

- an encryption unit that is subordinated to the analyzing unit, which is designed for

interchanging or removing of information components in the original amount of data or attaching of an information components at a predetermined position in the sequence of information components or exchanging of an information component with an information component that is preferably not contained in the original amount of data and

creating an amount of key data with information about the interchanged, removed, attached or exchanged information components, which are designed in a manner, that a reconstruction of the original amount is permitted with key data, and

- a storage unit which is designed to store the amount of key data in a key data storage unit and
- a volume data storage unit, which is designed to store the amount of, encrypted data.

14. Apparatus as set forth in claim 12, characterized in that the encryption unit is assigned to an equivalence unit, which provide at least one information component in the original amount of data for at least one equivalent information component, that is electronically stored, whereby the equivalent information component is designed in a manner, that it match with the corresponding information component grammatically, metaphorically, syntactically or regarding its format.

15. Apparatus as set forth in claim 14, characterized in that the encryption unit is designed to 25 interconnect with a semantic rule-applying unit, so that the interchanging, removing, attaching or exchanging are arranged within the grammar, format, metaphoric or syntax and which are determined by the format- or structural data.

16. Apparatus as set forth in claim 12, characterized in that a random controller unit is 30 assigned to the encryption unit, in which the interchanging, removing, attaching or exchanging of single information components or sequences of information component are controlled by the encryption unit randomly, in particular in a non reproducible manner.

17. Apparatus as set forth in claim 12, characterized by an encryption parameter unit that is 35 subordinated to the encryption unit, and is designed for storing or inserting predetermined parameter for the interchanging, removing, attaching or exchanging by

the encryption unit, in particular regarding a depth of encryption given by a number of interchanging, removing, attaching or exchanging operations.

18. Apparatus as set forth in claim 12, characterized by a conversion unit that is subordinated to the encryption unit, and is designed for generating an electronic transferable volume data file for the amount of encrypted data and preferably an actively executable program- or script file for the amount of key data.
- 5 19. Apparatus as set forth in claim 12, characterized in that the encryption unit is designed to generate a plurality of an amount of key data, which comprise at least one of the key data does not provide the reconstruction of the original amount of data while combining with the amount of encrypted data, but which lead to an amount of data after the combining, that is matched with the original amount of data in a syntactically, grammatically or format-related manner.
- 10 20. Apparatus as set forth in claim 12, characterized in that the analyzing unit is subordinated to the encryption unit and is designed in a manner that the amount of key data comprise information about the exchanging - or interchanging given by information component used to interchange, remove, attach or exchange.

100 90 80 70 60 50 40 30 20 10